HIPAA
&
HITECH Changes

Office of Corporate Compliance

R. Brett Short, Chief Compliance Officer

March 2011

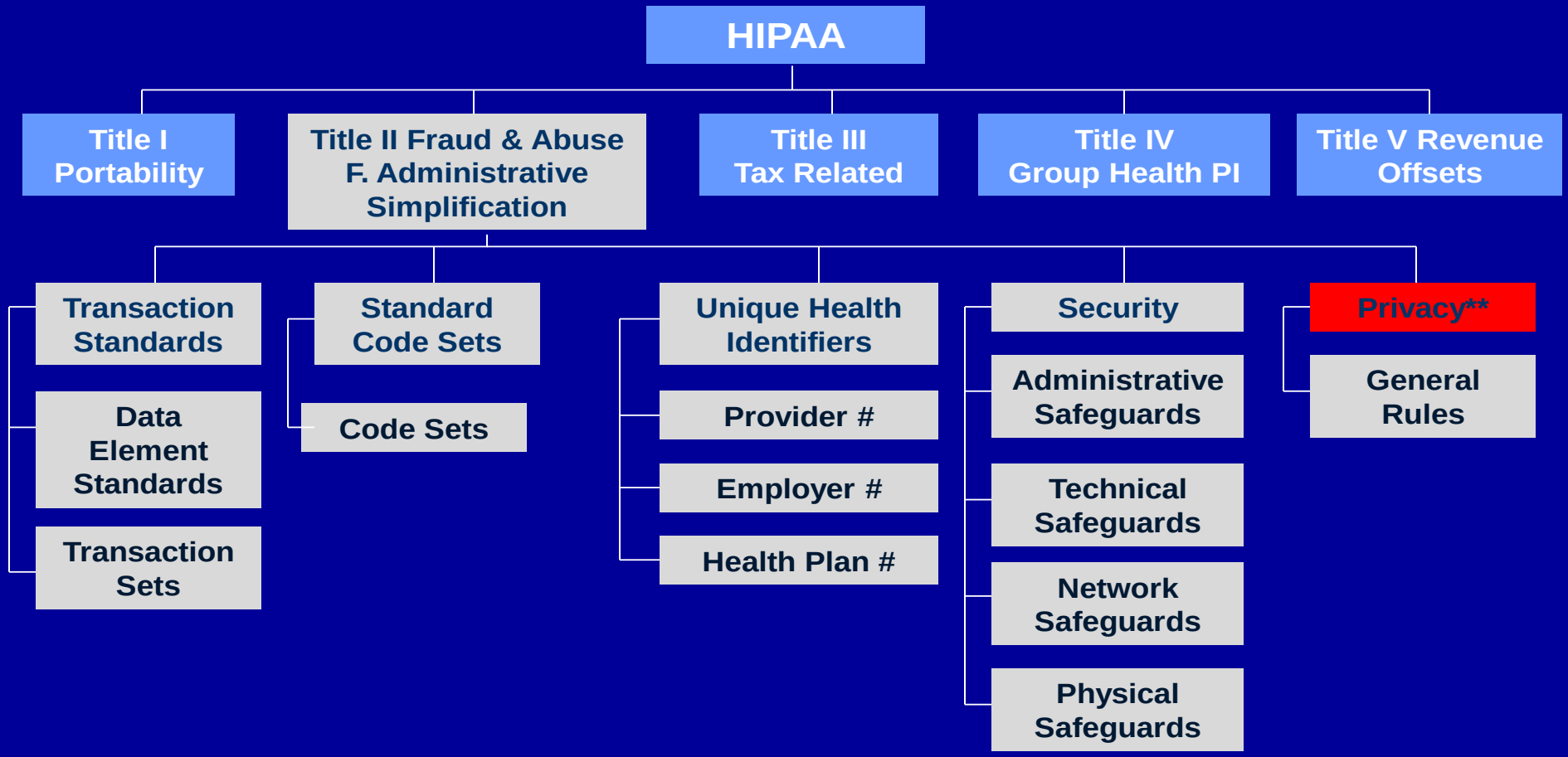
UKHealthCare

HIPAA & HITECH

- HIPAA
- HITECH Changes
- Business Associates
- Breach Notification

UKHealthCare

Background: HIPAA has many parts



UKHealthCare

Who is covered?

- Health Plans (Humana, Cigna, CHA, etc)
- Clearinghouses
- Providers that bill electronically
  - NEW – Business Associates of Covered Entities (2/17/09 – HITECH/ARRA)
  - Tool on the HHS/OCR website (https://www.cms.gov/apps/hipaa2decisionsupport/)

What is HIPAA

- Health Insurance Portability and Accountability Act
- 3 Uses:
  - Treatment
  - Payment
  - Operations (Accounting, education, planning, etc.)

What is PHI?

- Protected Health Information
- Any information including demographic data that relates to:
  - The individual's past, present, or future physical or mental health or condition
  - The provision of health care to the individual, or
  - The past, present, or future **payment** for the provision of health care to the individual

What information is protected?

- “individually identifiable health information”
  - Paper
  - Spoken
  - Electronic
  - Any media

UKHealthCare

HITECH/HIPAA

- Health Information Technology for Economic and Clinical Health (HITECH) Act,
  - passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

HITECH update

- Business Associates
- Request for Restrictions
- Minimum necessary
- Accounting for Disclosures
  - Applicability identification:
  - Pre- January 1, 2009? Current Users — Effective date Jan. 1, 2014 (1/1/16)
  - Post –January 1, 2009? New Users — Effective date Jan. 1, 2011 (1/1/13)

HITECH changes

- Electronic Access to Medical Records
- Sale of PHI from an EHR
- Marketing
- Health Care Operations

Timeline

Effective now - February 17, 2009:

- State Attorney General Provision
- Changes to enforcement provisions / Civil Monetary Penalties

April 18, 2009:

- Guidance on “Unsecure Protected Health Information”

August 17, 2009:

- HHS / FTC to issue interim Final Rule on Notification of Breaches for covered entities and PHR vendors
- September 16, 2009 (30 days past above) effective date for Breach Notification

December 31, 2009:

- Accounting of Disclosures standards (through rule-making procedures)

Timeline

February 17, 2010:

- Most Security provisions
- CEs will need BAA with PHRs, HIEs,
- Rules issued on Fundraising
- PHR guidance for privacy and security rules
- HHS to publish guidance on definition of Business Associates
- Request for Restrictions on items paid in full to health plans
- Electronic Access to records (electronic copy)

August 17, 2010:

- Minimum Necessary standard / LDS analysis
- Prohibition on sale of PHI
- Health Care Operations guidance

Timeline

Change in Accounting for disclosures

Delayed-

Sometime in 2011?

- Accounting of Disclosures for new users of EHR (after 1/1/2009)
- May be extended to 2013

Delayed - 2014

- Accounting of Disclosures for current users of EHR (before 1/1/2009):
- May be extended to 2016

Personal Health Records

1. Required to notify individuals if there is a breach of their unsecured IIHI
2. FTC notification
3. Third party service providers must notify PHR if they have a breach
4. Documentation of notification (same as CE)
    - Brief description of what happened
    - Unsecured PHI involved in Breach
    - Steps the individual should take to protect themselves
    - CE's investigation, mitigation of losses and corrective action plan
    - Platform for individuals to ask questions
5. *Need policy on Breach notification process, Secretary will issue guidance or ANSI If statute is addressing breach notifications for non-CEs is enacted, this will sunset.

Business Associates

- What is a Business Associate? - *A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.*
  - *A member of the covered entity's workforce is not a business associate.*
  - *A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.*

http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

Business Associates

- What is a Business Associate (continued) –
  - *Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.*
  - *Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.*
  - Examples above are for discussion, other circumstances exist

  See the definition of "business associate" at 45 CFR 160.103

Business Associates

- Why should providers care?
  - Relationship changes
  - Are you a BA or another CE?

Business Associates

- Application of Security Rule
- Application of the Privacy Rule
- Physical Safeguards
- Technical Safeguards
- Policies and Procedures
  - Many of these exists, CEs have had for some time
- Breach Notification
- Unsecure/Secure PHI
- Process or Policy identified

Business Associates

Action Items – for BAA requirements

1. Identify and inventory BAAs
   Develop a communication piece to discuss:
   -Breach Notification
   -Accounting for disclosure process

2. Identify situations where clinic/hospital/med center is a BA of another entity

a. Research?
b. State of KY?
c. Others?

Breach Notification

- “Unsecured PHI”
- Number of patients is important
- 60 days to notify
- Logged on HHS website
- 80% involve laptops
- Encryption

Summary

- HIPAA has more teeth
- AG can now bring suit against providers (share portion with patient)
- More rights for patients
- More liability for providers
- Report PHI breach immediately!

Who are your friends?

- Facebook
- Twitter
- MySpace
- Tweetdeck
- Social Media in general

Who you should “friend”:

- Public Relations/point person
  - Good to have prepared statements, situation specific
  - Be able to explain your privacy program
- Legal
- Marketing
- Customer Service
- IT/IS

Issues to Consider

- Handhelds/Mobile Media
  - mobile-PHI, must be protected
- Sign off the system when finished
- Social Media
- Email – Must be secured
- Privacy/Security Incidents
  - Report Immediately

Recent Enforcement

- February 23, 2011: HHS imposes a $4.3 Million Civil Money Penalty for Violations of HIPAA
  - Maryland Hospital
  - Refused to cooperate
  - Willful Neglect
  - *"Ensuring that Americans' health information privacy is protected is vital to our health care system and a priority of this Administration. The U.S. Department of Health and Human Services is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule,"* said HHS Secretary Kathleen Sebelius

Recent Enforcement

- February 24, 2011: Massachusetts Hospital settles potential HIPAA violations
  - $1 Million
  - Loss of 192 patient's data
  - Patient schedule
  - *"We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information,"* said OCR Director Georgina Verdugo.

Thank You

Office of Corporate Compliance

Brett Short, Chief Compliance Officer

Privacy Officer – Lynn Crothers

323-8002

Comply Line 1-877-898-6072

UKHealthCare